United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: System of Registries (SoR)	
Preparers: Todd Holderman, Dwayne Aydlett & Carroll Rich	**Office:** OMS/OIM/DMSD
Date: 03/03/2021	**Phone:** 202-566-2076, Holderman.Todd@epa.gov 202-566-1787, Aydlett.Dwayne@epa.gov 703-895-3150, Rich.Carroll@epa.gov
Reason for Submittal: New PIA____ Revised PIA____ Annual Review_X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

A Registry is not a storehouse of the information assets themselves. Instead, it contains information about the assets such as what they are, where to find them and how to use them. The System of Registries, also known as SoR, is an EPA major application. SoR was developed in and has been operational since 1995. SoR provides a gateway and search capability to several registries and repositories residing in the EPA OMS. These registries comprise an important link in EPA's information architecture and provide support to the National Environmental Information Exchange

Network. Specifically, the SoR was developed to support the Agency's data standards program and numerous Agency information technology initiatives, including the Agency architecture and data exchange with stakeholders through network nodes.

SoR collects metadata information. It contains information which makes EPA data accessible and understandable. This provides the ability to register, map, and manage information important to EPA and its partners. Registries like the Facility Registry and the Substance Registry maintain information about business objects common throughout EPA. The SoR is moving toward a web services and API architecture that allows applications or interfaces to be built using registry data. RegFinder is an application/interface to the Laws and Regulations Services (LRS) that allows users to search environmental laws and regulations through a browser-based interface while the data is maintained securely on EPA IT infrastructure.

This current revision to SoR PIA changes the last bullet under section 2.1 from "AWS cloud environment" to "EPA's cloud environment." There is no change to the RegFinder application/interface or the data served to it from the LRS.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The first registry within the System of Registries was a data registry that contained the metadata (data about data) describing standard and programmatic data elements found in EPA systems and applications. Next, a system inventory was created for centralizing the metadata about EPA systems and applications. This inventory evolved into the "official" EPA system list (READ - the Registry for EPA Applications, Models and Datasets), and is used for many purposes. Other specialized registries for lists of chemicals and facilities were added over time. A terminology registry, similar to a dictionary, was also incorporated to better service the need for supporting data transfer and transformation. Other registries managed by DMSD includes The Laws and Regulations Service, The North American Industrial Classification System registry, and the Enterprise Vocabulary.

Policy, Procedures and Standards

- Title III of the E-Government Act of 2002, Federal Information Security Management Act (FISMA)- 44 U.S.C.
- The Privacy Act of 1974, PL 93-579, as amended-5 U.S.C.; 552a
- The Freedom of Information Act, PL 93-502-5 U.S.C.; 552
- The Federal Managers' Financial Integrity Act (FMFIA), PL 97-255-31 U.S.C.; 3512
- OMB Circular A-130, Management of Federal Information Resources
- OMB Circular A-123 Revised, Management's Responsibility for Internal Control, December 2004

- OMB Circular A-127, Financial Management Systems, July 23, 1993
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. The current ATO Extension will expire November 12th 2023.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

A Registry is:

A directory to EPA metadata services and information. It contains information which makes EPA data accessible and understandable. The System of Registries (SoR) does not collect data – SoR collects information about agency systems.

•The specific data elements are work email, work phone number and name, and these date elements are derived from EIAM.

•SoR is the collection of registries.

- Individuals enter the metadata about their objects by logging into the registries or by sending the metadata to SoR personnel.
- READ collects information about systems existence, technology, architecture, etc.
- RCS collects similar information to READ but for many different types of resources, like APIs, web services, dataflows, widgets, software tools, etc.
- SRS collects information about chemicals and some biological substances
- FRS collects information about facilities of environmental interest
- TS collects information about terms, vocabularies, glossaries, etc.
- LRS manages the names of laws and regulations.
- TRIBES manages tribal names.
- REGFINDER enables searches of LRS and SRS – neither of which contain PII. REGFINDER does not collect information nor is any information directly accessible to REGFINDER users. REGFINDER is deployed in EPA's cloud environment.

2.2 What are the sources of the information and how is the information collected for the system?

SoR information is collected from applicable IT System metadata.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. SoR data comes from EPA systems and other Federal Agency systems.

2.4 Discuss how accuracy of the data is ensured.

OMS work with the EPA System Owners and other Federal Agency System Owners to ensure the accuracy and currency of the SoR data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

PII data collected is public record. Name, work email and work phone are collected in the system and use to identify an individual. Therefore, the risk level is low. Collection of inaccurate data will pose a low risk.

Mitigation:

A low risk of collecting inaccurate data is mitigated by identifying errors, and programs informed as appropriate.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Work email, work phone and name are accessible only after login except for those instances when contact information is important for public access.

SoR maintains user Roles and uses Least Privilege to mitigate proper authorization security controls.

SoR User Roles:

•Requester: person who enters the metadata – only user id is recorded, no other information requested or recorded.

•Owner: owner of the resource – no special rights, only name is necessary.

•Steward: only one who can make changes to metadata - usually is main contact – phone number or email address required.

•Contact: additional contact - no special rights, only name is necessary.

•Technical Contact: no special rights, only name is necessary.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access control Policy and Procedures: CIO 2150-P-01.2

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

All SoR users have accounts in the Agency Enterprise Identity Access Management (EIAM). Both internal and external users have access to SoR.

Yes, contractors have access to the system with appropriate FAR clauses in their contracts.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The EPA record Schedule number is 0096. Information is kept till it is obsolete.

Auditable events are described as the ingestion of records into the repository and the scheduled disposition of records from the system based on pre-defined records retention schedules. These events are audited on a weekly basis by reports generated from the NHS system. All deletions from the system are audited. The addition of records to the system is audited through weekly transaction reports and daily records transmission reports. The reports are maintained by the NCC NHS system administrator and the EPA NHS Program Management Office.

Documentation:

EPA's auditing policies are documented in:

• EPA Order 2195A1. (See the note in the Security Control, AU-1)

• Agency Network Security Policy OTOP 200.03

• Systems Engineering Monitoring and Log Review Procedures

• Standard Configuration Documents

• Monthly security Scan Results

• Support of IG Criminal Investigations

• UNIX and Windows Security Checklists

• Systems Engineering Policy on Security Scanning.

Directives/Procedures

•Records Management Policy (CIO 2155.3) February 10, 2015

This Policy establishes principles, responsibilities and requirements for managing EPA's records to ensure that the Agency is in compliance with federal laws and regulations, EPA policies and best practices for managing records.

•Records Schedules

EPA's official policies on how long to keep Agency records (retention) and what to do with them afterwards (disposition).

•Essential Records Procedures (EPA 2155.P-01.0) March 24, 2015

These procedures prescribe the requirements and responsibilities for establishing and maintaining EPA's vital records program.

https://www.epa.gov/records/epa-records-schedules-detailed-information

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

A privacy risk is that there is a low risk that information could be kept longer than needed.

Mitigation:

Record schedule is strictly followed.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No. The System of Registries supports EPA's business by contributing to its architecture, system development, and the EPA's ability to understand and exchange environmental information among its various programs and with its partners. The System of Registries will help promote reuse of data, metadata, and Service Oriented Architecture (SOA) components. The scope of information sharing does not apply to meta-data.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A.

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

No, there is no information sharing.

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security

measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The processes and controls described above outline how the system ensures information is used in accordance to stated practices in this PIA. The meta-data information used is not privacy data. It is publicly available information. Information is used for intended purposes in which it was collected and this can be ensured by reviewing system audit functions as needed to know who and how information is used.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Training is given to SoR managers on how to properly vet new user registrations, and how to use EPA's EIAM user management functions. The data is publicly available information. Also, SoR relies on EPA's Information Security and Privacy Awareness Raining for users.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Name, work phone and work email are available on the non-public version of SoR. Exceptions are when the contact information is important for public access. Also, if audits are not done timely and/or if done improperly could pose a risk.

Mitigation:

Name, work phone and work email are available on the non-public version of SoR. Exceptions are when the contact information is important for public access. An individual will only have access to these data elements only when they have been authenticated into the system. Another mitigation is to ensure there is a timely and appropriate system audit process in place to account for all data elements.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

SoR supports data quality and information management at the EPA.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes__ No_X__. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

The primary way information is retrieved from the SOR is through the use of substance identifiers which include both unique numbers and unique names for each substance and

chemical name. Information is retrieved for example, by chemical name, program name, system name, and environmental term. Information is not retrieved by personal identifier.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

Name, work phone and work email are available on the non-public version of SoR. Exceptions are when the contact information is important for public access. An individual will have access to these data elements only when they have been authenticated into the system

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Name, work phone and work email are available on the non-public version of SoR. Exceptions are when the contact information is important for public access. Low risk (not privacy risk related) of inappropriate use of individual contact information. No privacy risk related because SOR data is primarily scientific in nature.

Mitigation:

Name, work phone and work email are available on the non-public version of SoR. Exceptions are when the contact information is important for public access. An individual will only have access to these data elements only when they have been authenticated into the system. Ensure there is a timely and appropriate system audit process in place to account for all data elements. SoR relies on audit function to determine appropriate use.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: